arabelle solutions
EDF GROUP

August 27, 2025, **CYBERSECURITY**

Topic: VMware ESXi / Workstation Pro Multiple Vulnerabilities

Overview:

Several vulnerabilities, based on the VMWare operating systems ESXi & Workstation Pro have been published by the supplier VMWare / Broadcom in their security bulletin:

- **VMSA-2025-0004 (04/03/2025):** https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390

Arabelle Solutions has identified several products that include an impacted VMWare version, listed below:

Affected Versions:

- VMware ESXi: Versions 7.0
- VMware ESXi: Versions 8.0
- VMWare Workstation Pro: Versions 17.x

Impacted Products:

- Mark VIe OT Armor Security
- Cyber Jump Station (Secure Remote Connection)
- Cyber Alspa Security Server
- Alspa Controcad with Virtual Machines
- Alspa Virtualization Server
- Digital Product KPE Server

Identified risks:

CVE-2025-22224 - Vulnerability Details – VMCI heap-overflow vulnerability
CVSSv3 Score: 9.3 (High)
A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.

CVE-2025-22225 - Vulnerability Details – VMware ESXi arbitrary write vulnerability
CVSSv3 Score: 8.2 (High)
A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox.

CVE-2025-22226 - Vulnerability Details – VMware ESXi arbitrary write vulnerability
CVSSv3 Score: 7,1 (High)
A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the VMX process.

Mitigation:

There is no specific mitigation or workaround given by the supplier VMWare / Broadcom to cover these three vulnerabilities. Their only proposal is to update the software.

However, if the update is not possible, some compensatory measures and basic rules could be put in place about access to virtual machines:

- Physically, the server host must be:
  - in a room with restricted and authorized access,
  - in a locked cubicle with restricted access
- Password management for computer access must be done by the project with very strong confidentiality,
- Administration passwords must meet complexity requirements,
- If possible, keep only one account for administration with administrator rights.

Remediation:

The solution given by the supplier is the upgrade of the product:

Product	**Version**	**Fixed Version**
ESXi	**8.0**	**ESXi80U3d-24585383 (8.0 Update 3d)**
ESXi	**7.0**	**ESXi70U3s-24585291 (7.0 Update 3s)**
Workstation	**17.x**	**17.6.3**

Defense-in-depth:

To minimize the risk of the exploitation of current and future system vulnerabilities, Arabelle Solutions highly recommends implementation of a defense-in-depth strategy (complementary defenses in Physical, Technical, and administrative domains) for your critical process control systems.

We will be pleased to support you in the enhancement of your cybersecurity strategy and improve or update your current equipment with latest cybersecurity methodologies and solutions. We suggest that a thorough analysis of your cybersecurity status be performed and resulting recommendations for an optimal solution be implemented according to the level of risk exposure and/or the standard frameworks which are applicable to your needs.

Contact your Arabelle Solutions Automation & Controls Sales person or our Help Desk at +33 1 60 10 01 30 / helpdesk-control-systems@arabellesolutions.com for help with ordering cybersecurity services and solutions.

Revision History

Version	**Release Date**	**Purpose**
A	August 27, 2025	Initial version